

Comments to the Copyright Office
on DMCA Anti-Circumvention Provisions

Mr. David O. Carson
Office of the General Counsel
Copyright Office GC/I&R
P.O. Box 70400
Southwest Station
Washington, D.C. 20024
Sent via email: 1201@loc.gov

Mr. Carson:

I must first offer thanks to the office for hearing these comments. I must also state that the opinions expressed are my own, and not necessarily held by my employer or fellow employees, although several of them have expressed comments similar to mine.

As a researcher at a university investigating new and alternative methods of digital content transfer and delivery, I find several of the comments within the DMCA cumbersome and distasteful.

I agree with the comments sent to you by the Electronic Frontier Foundation by Robin D. Gross on Feb 17, 2000. I find their comments about the CSS and DeCSS reason enough to make changes to the anti-circumvention provisions within the act. I will also attempt to answer the questions as outlined.

Questions 1 and 2--

There are many methods for protecting works which I have studied -- many more than I can mention. For digital works, these typically include one or more methods of encryption, obfuscation or otherwise making unreadable useful sections of information, separation of content among multiple sources requiring partial or full knowledge of the sources to reconstruct the useful information, and mingling 'chaff' or otherwise useless information among the valid information, requiring external knowledge to reconstruct or remove or 'winnow' the chaff, just to name a few.

In order to lawfully reconstruct the information, the viewer must be able to decode the information, or somehow be able to extract from it enough information

to generate a useful signal. The different methods and measures taken to secure the work make substantial differences in the methods that must be taken in archival of said works.

The CSS protection system is an example of one of these methods, and it has achieved much popularity. It essentially uses encryption to protect the work, requiring knowledge of both the encryption system used and the protecting key required by the system in order to decode the data. While this allows viewing on a particular system, it does not preclude the illegal copying of the data while in its encoded form, nor does it allow the legal viewing on systems where there does not exist any authorized form of viewing. This in turn makes it illegal for people to use their property for legal uses.

Systems which transmit the legally decoded information in a useable form across any type of open network where the information may be decoded might be considered a method of circumventing that protection system if the information is intercepted at any point along that open network. While the interception of the information is already covered by existing law, the DMCA would have the network owner or the transmitter responsible if the person had any knowledge that they system might be insecure. Open networks are inherently insecure, as clearly indicated in research in that area. I fear that this area of research, specifically the legal broadcast or multicast (= sending a signal to multiple, identified persons) of copyrighted information, may fall prey to various interpretations of this law.

Questions 3 through 7--

Again, many various protection systems exist which are applied and exist only electronically and through technological means. A great deal of research done around the globe and in countless publications enumerate specific products, each of which exist in these forms; enumeration of these systems would be impossible except on a very large scale. Several document encoding systems rely upon the rendering system being attached to the Internet or other network to ensure proper payment for viewing time, any printouts made, etc. Many of these systems are employed only on a single platform or on a single system. While an individual or group may wish to translate them to work properly on a native system, I fear that this act will prevent the lawful use of the protected system by disallowing the legitimate translation of an authorized system to an unauthorized platform -- even if the security systems remain intact.

Questions 8 and 10--

Among the various methods of storing our large data source, we have examined the purchase and use of DVD technology. The purposes here are clearly within the bounds of both research and education of other researches, and the long-term

and inexpensive archival of our data. In our lab we use the Linux operating system (along side the HPux, Windows, IRIX, and other systems) for which no properly authorized DVD or CD interpreters exist. While many people are not aware of this, CD-ROMs also have built-in security which is trivial to avoid, and because so many systems violate the security, they are largely ignored as protected devices. By reading or writing to either of these storage systems while on this platform, we will be violating the DMCA, and therefore are limited to the platforms which are authorized through the expensive authorization methods to support these formats, specifically the Microsoft platform only. This is contrary to the purpose of our lab, which is not to be tied to a specific platform.

Therefore this law, under some interpretations, may not only restrict our educational purposes, it may stop them completely. It also encourages the use of a single manufacturer, essentially legally mandating that a particular company provide the service and denying it to all others, as companies have been attempting to do for years.

Questions 9, 11, 12, 13, 14, 27, 29--

There is much criticism in our own lab and with others about the lawsuits being filed regarding groups such as iCraveTV.com, and DeCSS, including the (in our opinions) improper way that United States Law was executed outside our borders due to pressures from corporations and businesses. I believe that the EFF and other related comments in this area ought to be carefully considered.

I fear that many existing technically based systems and many being designed in new research will be misused, or that a variant on our research will be applied in such a way that lawsuits will be filed against us because a criminal used our tools in a manner which violated existing law. Two specific instances where I believe hardship has occurred due to this Act are in the iCraveTV.com lawsuit, and in the various lawsuits regarding DeCSS. I do not know of others which have progressed beyond threat of lawsuits, but I know that interpretation of this law will certainly damage the developers of systems because the users of the system choose to misuse or abuse them.

Again, I fear that interpretations of the law may preclude our otherwise lawful use of using digital medium for storage, archival, and research use, especially in these areas. Simply because content is copyrighted, if there exists the possibility that proper use of a system is legal and misuse of the system is unlawful, we should not improperly limit their use, instead we should encourage more research and education, not just in academic and research facilities, but

in all areas.

For examples, while copy machines and printers can be used duplicate copyrighted material, it may do these things within or without the scope of the law.

Similarly, transmission technologies may transfer information lawfully or unlawfully. The medium itself should not be limited, but the act of violating the law should be limited. I fear that the DMCA is attempting to regulate the copy machines and the broadcast wires rather than regulate the persons violating the law.

I urge you to consider that the technology, the protocols and systems, the medium used or the method of transfer are NOT the cause of the problem. The problem is the criminals who are using the systems to violate existing law. If you choose to further restrict the technology, you will not be solving the problem.

Restricting the technology will drive the costs of research up, because researchers will be spending more money investigating the laws, and possibly less on the products, thereby driving down quality and increasing costs. Restricting the technology will drive small businesses and individual researchers out of the field, lowering competition and again damaging consumers.

I will ask you to consider that other citizens of other nations often laugh at the restrictions placed on technology research here in the United States. It is not an uncommon discussion in any large group of citizens. Please do not cause further embarrassment to our nation by ignoring the benefits that new technology gives, or by cutting the throats of small businesses and private researchers, who do not have the time or money to fight large companies in expensive lawsuits designed to eliminate their competition.

Finally, I ask you to go back and reread the source of our governments power, that is the United States Constitution, where the power is granted to congress to enact laws to ENCOURAGE THE DEVELOPMENT of the arts and sciences and PROTECT THE RESPECTIVE ARTISTS AND RESEARCHERS, not to restrict the development and use of advanced technologies to large businesses, providing only pre-packaged and stale technology to others in our land. I ask that the findings you present be just that, to ENCOURAGE and PROTECT development, not to DISCOURAGE and PROSECUTE those who have new ideas.

Sincerely,

Bryan Z. Wagstaff
bryanw@cs.byu.edu
bryanw@xmission.com
888 N 600 W #45
Provo, UT 84604